RECEIVED
CENTRAL FAX CENTER
MAR 2 1 2007

AMENDMENTS TO THE CLAIMS

• Please amend the claims as follows:

1. (cancelled) ~~The method of claim 9, comprising the steps of:~~

~~generating a plurality of random numbers;~~

~~distributing in a digital medium the plurality of random numbers to the members of the group;~~

~~publishing a hash value of contents of the digital medium;~~

~~distributing to the members of the group public-key encrypted messages each containing a same token comprising a random number; and~~

~~encrypting a message with a key generated from the token and the plurality of random numbers.~~

2. (currently amended) The method of ~~claim 1~~ claim 9, wherein the generating step comprises generating at least approximately 20,000 random numbers.

3. (original) The method of claim 2, wherein the generating step comprises generating 256-bit random numbers.

4. (currently amended) The method of ~~claim 1~~ claim 9, wherein the step of distributing in a digital medium comprises distributing in a removable digital medium.

5. (original) The method of claim 4, wherein the step of distributing in a digital medium comprises distributing in a medium selected from the group consisting of CD-ROMs and DVD-ROMs.

6. (currently amended) The method of ~~claim 1~~ claim 9, wherein the steps of publishing a hash value comprises employing a Secure Hash Algorithm.

7. (currently amended) The method of ~~claim 1~~ claim 9, additionally comprising the step of rejecting a digital medium received by a user if a hash value of contents of the received digital medium does not equal the published hash value of the contents of the distributed digital medium.

8. (currently amended) The method of ~~claim 1~~ claim 9, wherein the step of distributing a token is performed daily.

9. (previously presented) A method of performing electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, the method comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group;

publishing a hash value of contents of the digital medium;

distributing to the members of the group public-key-encrypted messages each containing a same token comprising a random number; and

encrypting a message with a key generated from the token and the plurality of random numbers;

wherein the step of distributing a token comprises distributing a verification message comprising an element for each user, each element comprising the token encrypted with the corresponding user's public key, and the method additionally comprises the step of publishing a hash value of the verification message.

10. (original) The method of claim 9, additionally comprising the step of rejecting a token received by a user if a hash value of a received verification message does not equal the published hash value of the distributed verification message.

11. (original) The method of claim 10, additionally comprising the step of rejecting a token received by a user if every element of the verification message does not equal the received token encrypted with the corresponding user's public key.

12. (currently amended) The method of ~~claim 1~~ claim 9, wherein the encrypting step comprises employing symmetric key encryption.

13. (currently amended) The method of ~~claim 1~~ claim 9, wherein the encrypting step comprises choosing randomly one of the plurality of random numbers.

14. (original) The method of claim 13, additionally comprising the step of sending the encrypted message with an index to the randomly chosen number and a timestamp sufficient to enable a recipient to determine a proper decryption token.

15. (currently amended) The method of ~~claim 1~~ claim 9, wherein the group is a domain.

16. (currently amended) The method of ~~claim 1~~ claim 9, wherein one or more members of the group is a domain.

17. (currently amended) The method of ~~claim 1~~ claim 9, wherein anonymity of a sender of the message is maintained.

18. (previously presented) A method of performing electronic communications between members of a group wherein the communications are authenticated as being from a member of the group and have not been altered, the method comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group;

publishing a hash value of contents of the digital medium;

distributing to the members of the group public-key-encrypted messages each containing a same token comprising a random number; and

encrypting a message with a key generated from the token and the plurality of random numbers;

wherein anonymity of a sender of the message is maintained; and

additionally comprising the step causing the encrypted message to be transmitted over a network such that a recipient of the encrypted message receives no data concerning network routing of the encrypted message.

19. (original) The method of claim 18, wherein the step causing the encrypted message to be transmitted over a network comprises employing onion routers.

20. (original) The method of claim 19, wherein employing onion routers comprises encrypting messages received by the onion routers with a public key of the recipient.

21. (currently amended) The method of ~~claim 1~~ claim 9, wherein the method provides absolute anonymity for communications between the members.

22. (previously presented) The method of claim 21, wherein the method provides anonymity as to authorship of the communications and as to electronic mail routing of the communications.

23. (currently amended) The method of ~~claim 1~~ claim 9, wherein the method provides anonymity for communications between the members by not providing for communications between members of the group within a same domain.

24. (previously presented) A method of performing electronic communications between members of a group wherein the communications are authenticated as being

from a member of the group and have not been altered, the method comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group;

publishing a hash value of contents of the digital medium;

distributing to the members of the group public-key-encrypted messages each containing a same token comprising a random number; and

encrypting a message with a key generated from the token and the plurality of random numbers;

wherein the method provides relative anonymity for communications between the members; and

wherein anonymity is not provided for communications between members of the group within a same domain.

25. (previously presented) The method of claim 24, comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group; and

encrypting a message with a key generated from a token and the plurality of random numbers while maintaining anonymity of authorship of the message.

26. (previously presented) The method of claim 24, comprising the steps of:

generating a plurality of random numbers;

distributing in a digital medium the plurality of random numbers to the members of the group;

encrypting a message with a key generated from a token and the plurality of random numbers; and

permitting revocation of the message by a revocation authority comprising one or more of the members.

27. (original) The method of claim 26, wherein the permitting step maintains anonymity of authorship of the message.